Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0438-2007

for

S3CC9GC 16-Bit RISC Microcontroller for Smart Card, Version 11

from

Samsung Electronics Co., Ltd.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0438-2007

S3CC9GC 16-Bit RISC Microcontroller for Smart Card, Version 11

from

Samsung Electronics Co., Ltd.

Common Criteria Arrangement for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Version 2.3* (ISO/IEC 15408:2005) extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

PP Conformance:	**Protection Profile BSI-PP-0002-2001**
Functionality:	**BSI-PP-0002-2001 conformant plus product specific extensions Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant**, **EAL4 augmented by:** ALC_DVS.2 (Life cycle support - Sufficiency of security measures), AVA_MSU.3 (Vulnerability assessment - Analysis and testing for insecure states), ADV_IMP.2 (Implementation) AVA_VLA.4 (Vulnerability assessment - Highly resistant)

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 01. March 2007

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

Part A: Certification
Part B: Certification Results
Part C: Excerpts from the Criteria
Part D: Annexes

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), version 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective in March 1998. This agreement has been signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognizes certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC. As of February 2007 the arrangement was signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America.

The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product S3CC9GC 16-Bit RISC Microcontroller for Smart Card, Version 11 has undergone the certification procedure at BSI. For this evaluation specific results from the evaluation process based on BSI-DSZ-CC-0400-2007 were re-used.

The evaluation of the product S3CC9GC 16-Bit RISC Microcontroller for Smart Card, Version 11 was conducted by TÜV Informationstechnik GmbH. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

Samsung Electronics Co., Ltd.
San24, Nongseo-dong, Giheung-gu, Yongin-City, Gyeonggido
449-711, Korea

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 01. March 2007.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-24 and D-1 to D-4.

The product S3CC9GC 16-Bit RISC Microcontroller for Smart Card, Version 11 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 (0)3018 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] Samsung Electronics Co., Ltd.
San24, Nongseo-dong, Giheung-gu, Yongin-City, Gyeonggido
449-711, Korea

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1	Executive Summary	3
2	Identification of the TOE	11
3	Security Policy	12
4	Assumptions and Clarification of Scope	13
5	Architectural Information	14
6	Documentation	14
7	IT Product Testing	14
8	Evaluated Configuration	16
10	Results of the Evaluation	16
10	Comments/Recommendations	19
11	Annexes	20
12	Security Target	20
13	Definitions	20
14	Bibliography	23

1 Executive Summary

The product type of the Target of Evaluation (TOE) is the S3CC9GC 16-Bit RISC Microcontroller for Smart Card, Version 11.

For this evaluation specific results from the evaluation process based on BSI-DSZ-CC-0400-2007 were re-used. The TOE, the S3CC9GC microcontroller featuring the TORNADO™ cryptographic co-processor, is a Smart Card integrated circuit which is composed of a processing unit, security components, contactless and contact based I/O ports and volatile and non-volatile memories (hardware).

The TOE comprises the hardware of the smart card security controllers, type S3CC9GC and IC Designer/Manufacturer proprietary IC Dedicated Software required for operation. Such software (also known as IC firmware) is mainly used for testing purpose during production only but also provides additional services to facilitate the usage of the hardware and/or additional services including a RSA asymmetric cryptography library and an AIS20 [4] compliant random number generation library. All other software is called Smart Card Embedded Software, which is not part of the TOE.

Regarding the RSA crypto library the user has the possibility to tailor this IC Dedicated Software part of the TOE during the manufacturing process by deselecting the RSA crypto library. Hence the TOE can be delivered with or without the functionality of the RSA crypto library what is resulting in two TOE configurations. If the user decides not to use the RSA crypto library the library is not delivered to the user. In this case, Rivest-Shamir-Adleman (RSA) is not provided by the TOE. Deselecting the RSA crypto library means excluding the code implementing functionality, which the user decided not to use. Excluding the code of the deselected functionality has no impact on any other security policy of the TOE, it is exactly equivalent to the situation where the user decides just not to use the functionality.

The TOE S3CC9GC is manufactured in IC fabrication of Samsung in Giheung, Korea, indicated by the production line indicator “14” as hex (see part D, Annex A of this report).

The hardware part of the TOE is the complete chip, composed of hardware and software parts.

- The TOE hardware consists of 72K bytes EEPROM, 6K bytes RAM, 2K bytes Crypto RAM, 256K User ROM, 12K Test ROM, 16-bit Central Processing Unit (CPU), Internal Voltage Regulator (IVR), Detectors & Security Logic, a non-deterministic random number generator (RNG, this non-deterministic part is only tested according to seed generation for conformance to AIS20 [4]), Memory Protection Unit (MPU), Triple DES cryptographic coprocessor with 112 or 168 bits key size, AES cryptographic coprocessor with 128 bits, 192 bits and 256 bits key size, TORNADO™ modular multiplier supporting up to 2048-bit RSA, Hardware UART for

contact and contactless I/O modes (Radio Frequency power and signal interface (RF Interface), Address & data buses, Internal Clock and Timers.

- The TOE firmware and software consist of Test ROM code (that is used for testing the chip during production), the TORNADO RSA secure cryptographic library v3.5S (optional), a Deterministic Random Number Generator (DRNG) that fulfils the requirements of AIS20.

The functions of the library included in the TOE are TND_RSA_SigSTD_Secure (RSA signature generation with straightforward method), TND_RSA_SigCRT_Secure (RSA signature generation with CRT method), TND_RSA_SigCRT_Secure3 (RSA signature generation with CRT method), TND_RSA_Verify (RSA signature verification) and RSA_Key_Generation (RSA key generation). The library supports operation size from 32 bits to 2048 bits by step of 2 bits. However, only key sizes from 1024 bits up to 2048 bits are within the scope of this evaluation.The Smart Card Embedded Software is not part of the TOE (for more details see Security Target [7]).

The TOE is intended to be used in a range of high security applications like banking and finance applications, communication highways (Internet access and transaction processing), Transport and ticketing applications (access control cards) and Governmental cards (ID cards, health cards, driving licenses). Several security features independently implemented in hardware or controlled by software will be provided to ensure proper operations and the integrity and confidentiality of stored data. This includes measures for memory protection, leakage protection and sensors to allow operations only under specified conditions.

The Security Target is written using the Smart card IC Platform Protection Profile, Version 1.0, July 2001, BSI registration ID: BSI-PP-0002-2001 [9]. With reference to this Protection Profile, the smart card product life cycle is described in 7 phases. The development, production and operational user environment are described and referenced to these phases. TOE delivery is defined at the end of phase 3 as wafers.

The assumptions, threats and objectives defined in this Protection Profile [9] are used. To address additional security features of the TOE (e.g cryptographic services), the security environment as outlined in the PP [9] is augmented by an additional policy, an assumption and security objectives accordingly.

The IT product S3CC9GC 16-Bit RISC Microcontroller for Smart Card, Version 11 was evaluated by TÜV Informationstechnik GmbH. The evaluation was completed on 26. February 2007. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

[8] Information Technology Security Evaluation Facility

The sponsor, vendor and distributor is

Samsung Electronics Co., Ltd.
San24, Nongseo-dong, Giheung-gu, Yongin-City, Gyeonggido
449-711, Korea

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL4+ (Evaluation Assurance Level 4 augmented). The following table shows the augmented assurance components.

Requirement	Identifier
EAL4	TOE evaluation: Semiformally designed and tested
+: ALC_DVS.2	Life cycle support – Sufficiency of security measures
+: AVA_MSU.3	Vulnerability assessment - Analysis and testing for insecure states
+: ADV_IMP.2	Implementation of the TSF (TSF: TOE Security Functions)
+: AVA_VLA.4	Vulnerability assessment - Highly resistant

Table 1: Assurance components and EAL-augmentation

Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from CC part 2:

Security Functional Requirement	Identifier	Source from PP or added in ST
FCS	**Cryptographic support**	
FCS_COP.1	Cryptographic operation	ST
FCS_CKM.1	Cryptographic key generation	ST
FDP	**User data protection**	
FDP_ACC.1	Subset access control	ST
FDP_ACF.1	Security attribute based access control	ST
FDP_IFC.1	Subset information flow control	PP
FMT	**Security Management**	
FMT_MSA.1	Management of security attributes	ST
FMT_MSA.3	Static attribute initialisation	ST

Security Functional Requirement	Identifier	Source from PP or added in ST
FMT_SMF.1	Specification of management functions	ST
FPT	**Protection of the TOE Security Functions**	
FPT_FLS.1	Failure with preservation of secure state	PP
FPT_ITT.1	Basic internal TSF data transfer protection	PP
FPT_PHP.3	Resistance to physical attack	PP
FPT_SEP.1	TSF domain separation	PP
FRU	**Resource utilisation**	
FRU_FLT.2	Limited fault tolerance	PP

Table 2: SFRs taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Identifier	Source from PP or added in ST
FAU	**Security Audit**	
FAU_SAS.1	Audit storage	PP / ST[9]
FCS	**Cryptographic support**	
FCS_RND.1	Quality metric for random numbers	PP / ST
FMT	**Security management**	
FMT_LIM.1	Limited capabilities	PP
FMT_LIM.2	Limited availability	PP

Table 3: SFRs CC part 2 extended

Note: Only the titles of the Security Functional Requirements are provided. For more details please refer to the Security Target [7], chapter 5.1 and 7.2.

These Security Functional Requirements are implemented by the TOE Security Functions:

TOE Security Functions	Description
SF1	Environmental Security violation recording and reaction
SF2	Access Control
SF3	Non-reversibility of TEST and NORMAL modes
SF4	Hardware countermeasures for unobservability
SF5	Cryptography

[9] PP/ST: component is described in the PP but operations are performed in the ST.

Table 4: TOE Security Functions

SF1: Environmental Security violation recording and reaction

This function records in registers the events notified by the detectors. The integrated detectors are frequency detector, voltage detector, temperature detector, light detector, inner insulation removal detector, active shield removal detector and power glitch detector. The filters integrated are used for preventing noise, glitches and extremely high frequency in the external reset or clock pad from causing undefined or unpredictable behavior of the chip.

SF2: Access Control

This security function manages access to the security control registers through access control security attributes. The user mode (NORMAL mode) has another function, which is write-enabled bit for security related registers. If the user does not enable this bit in 128 cycles after the reset, the user cannot write security control registers any more (for more details refer to the Security Target [7], chapter 6.1).

SF3: Non-reversibility of TEST and NORMAL modes

The NORMAL mode of the TOE consists of privilege mode and user mode. This function disables the TEST mode and enables the NORMAL mode of the TOE. This function ensures the non-reversibility of the Normal mode. This function is used once during the manufacturing process only (for more details refer to the Security Target [7], chapter 6.1).

SF4: Hardware countermeasures for unobservability

This function protects the memory and the address/data bus from probing attacks. This security function protects also the memory contents of the TOE from data analysis on the stored data as well as on internally transmitted data. The algorithms used for encryption are proprietary. The ROM scrambling is static key while the RAM and the EEPROM scrambling are dynamic key. RAM scrambling is performed automatically while EEPROM scrambling is defined and managed by the embedded software. The Central Processing Unit (CPU) of the TOE is synthesizable with glue logic, which makes reverse engineering and signal identification more difficult. Most sensitive hardware components such as buses are also hidden and implemented in deepest layers. The TOE operations can be made asynchronous by using the Internal Variable Clock and the Random Wait Generator security features. They make a full range of intrusive (e.g. probing attacks) and non intrusive attacks (e.g. side-channel attacks) more complex and difficult.

SF5: Cryptography

This function is used for encrypting and decrypting data using the Triple DES symmetric algorithm. A Random Number Generator is used for

generating random numbers for security processes in smart card applications and provides a mechanism to generate random numbers. It includes two functions: A random SEED Generation algorithm that generates a truly random number and a Deterministic Random Number Generator (DRNG) algorithm compliant with AIS 20 [4] (class K3 SOF High requirements). TORNADO RSA Cryptographic Library (optional) assists in the acceleration of modulo exponentiations required in the RSA encryption/decryption algorithm. TORNADO is a high speed modular multiplication coprocessor for RSA public key asymmetric cryptographic support. The TORNADO RSA Library is a software built for the TORNADO coprocessor it provides high level interfaces for RSA based algorithms (for more details please refer to the Security Target [7], chapter 6.1).

As the final transition from test mode to normal mode is performed before TOE delivery, all TOE Security Functions are applicable from TOE delivery at the end of phase 3 (except SF3).

1.3 Strength of Function

The TOE's strength of functions is claimed 'high' (SOF-high) for specific functions as indicated in the Security Target [7].

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The threats which were assumed for the evaluation and averted by the TOE and the Organisational Security Policies defined for the TOE are specified in the Security Target [7] and can be summarised as follows.

It is assumed that the attacker is a human being or a process acting on behalf of him.

So-called standard high-level security concerns defined in the Protection Profile [9] were derived from considering the end-usage phase (Phase 7 of the life cycle as described in the Security Target) as follows:

- manipulation of User Data and of the Smart Card Embedded Software (while being executed/processed and while being stored in the TOE's memories),
- disclosure of User Data and of the Smart Card Embedded Software (while being processed and while being stored in the TOE's memories) and
- deficiency of random numbers.

These high-level security concerns are refined in the Protection Profile [9] and used by the Security Target [6] by defining threats on a more technical level for

- Inherent Information Leakage,
- Physical Probing,
- Physical Manipulation,
- Malfunction due to Environmental Stress,
- Forced Information Leakage,
- Abuse of Functionality and
- Deficiency of Random Numbers.

Phase 1 and the Phases from TOE Delivery up to the end of Phase 6 are covered by assumptions (see below).

The development and production environment starting with Phase 2 up to TOE Delivery are covered by an Organisational Security Policy outlining that the IC Developer / Manufacturer must apply the policy “Protection during TOE Development and Production (P.Process-TOE)” so that no information is unintentionally made available for the operational phase of the TOE. The Policy ensures confidentiality and integrity of the TOE and its related design information and data. Access to samples, tools and material must be restricted.

A specific additional security functionality Triple-DES, Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA, if selected) must be provided by the TOE according to an additional security policy defined in the Security Target [7].

Objectives are taken from the Protection Profile plus additional ones related to the additional policy.

1.5 Special configuration requirements

The TOE has two different operating modes, *normal mode* and *test mode*. The application software being executed on the TOE can not use the *test mode*. The TOE is delivered as a hardware unit at the end of the IC manufacturing process (Phase 3). At this point in time the operating system is already stored in the non-volatile memories of the chip and the *test mode* is disabled.

Thus, there are no special procedures for generation or installation that are important for a secure use of the TOE. The further production and delivery processes, like the Smart Card Finishing Process, Personalisation and the delivery of the smart card to an end user, have to be organised in a way that excludes all possibilities of physical manipulation of the TOE.

There are no special security measures for the start-up of the TOE besides the requirement that the controller has to be used under the well-defined operating conditions and that the requirements on the software have to be applied as described in the user documentation and chapter 10 of this Report.

1.6 Assumptions about the operating environment

Since the Security Target claims conformance to the Protection Profile [9], the assumptions defined in section 3.2 of the Protection Profile are valid for the Security Target of this TOE. With respect to the life cycle defined in the Security Target, Phase 1 and the Phases from TOE Delivery up to the end of Phase 6 are covered by these assumptions from the PP:

The developer of the Smart card Embedded Software (Phase 1) must ensure:

- the appropriate “Usage of Hardware Platform (A.Plat-Appl)” while developing this software in Phase 1. Therefore, it has to be ensured, that the software fulfils the assumptions for a secure use of the TOE. In particular the assumptions imply that developers are trusted to develop software that fulfils the assumptions.
- the appropriate “Treatment of User Data (A.Resp-Appl)” while developing this software in Phase 1. The smart card operating system and the smart card application software have to use security relevant user data of the TOE (especially keys and plain text data) in a secure way. It is assumed that the Security Policy as defined for the specific application context of the environment does not contradict the Security Objectives of the TOE. Only appropriate secret keys as input for the cryptographic function of the TOE have to be used to ensure the strength of cryptographic operation.

Protection during Packaging, Finishing and Personalisation (A.Process-Card) is assumed after TOE Delivery up to the end of Phase 6, as well as during the delivery to Phase 7.

The following additional assumption is assumed in the Security Target:

- It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).
- All User Data are owned by Smart Card Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Smart Card Embedded Software as defined for the specific application context.
- The developer of the Smart Card Embedded Software must ensure the appropriate “Usage of Keydependent Functions (A.Key-Function)” while developing this software in Phase 1. Key-dependent functions (if any) shall be implemented in the Smart Card Embedded Software in a way that they are not susceptible to leakage attacks.

1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

S3CC9GC 16-Bit RISC Microcontroller for Smart Card, Version 11

The following tables outline the TOE deliverables:

No	Type	Identifier	Release	Form of delivery
1	HW	S3CC9GC	Vers. 11	Wafer
2	SW	DRNG	V2.0	Source code in electronic form
3	SW	Secure Crypto Library (optional)	V3.5S	Source code in electronic form
4	DOC	User's manual [11]	V3.1	In electronic form
5	DOC	Security Application Note [12]	V1.5	In electronic form
6	DOC	RSA Application Note [13]	V1.8	In electronic form
7	DOC	DRNG Application Note [14]	V2.0	In electronic form
8	DOC	S3CC9GC Delivery Specification [15]	V1.2	In electronic form

Table 5: Delivered documents of the TOE

The delivered micro chips contain the actual TOE and the embedded software. They are delivered in form of wafers from the TOE Manufacturer (logistics warehouse in Onyang) to the Card Manufacturer.

The TOE's confidentiality and availability should be protected during the delivery. The user software (operating system) will be loaded on the delivered TOE. Then the TOE is under the control of the user software and the TOE manufacturer (Samsung) can guarantee the integrity up to the delivery process.

A processing step during wafer testing incorporates the chip-individual features into the TOE. Each individual TOE is uniquely identified by its product code.

This product code in the EEPROM Security area is TOE specific as among others. It includes the core, application category, serial number, version, internal development code, and customer ROM code. It is described how the customer can retrieve this information. Each individual TOE can therefore be traced unambiguously and thus assigned to the entire development and production process (compare Table 6).

The TOE is identified by S3CC9GC revision 11. Another characteristic of the TOE is the product code. This information is stored in the EEPROM and can be read out by the user of the card via the normal EEPROM read command. It contains the following information at which among others the production line indicator is part of the serial number. Here the hex value “14” at the beginning of the serial number indicates that the TOE is produced in Giheung wafer line 5.

Address	Contents	Data
80000h – 80001h	Chip status information	Samsung’s internal management value
80002h – 80003h	ROM code number	ROM code number
80004h – 80005h	Device Type	100C h
80006h – 8000Fh	Available for customer	All FF h
80010h – 8001Bh	Serial number	Samsung’s internal management value beginning with 14 h
8001Ch – 8001Dh	IC Fabricator	4250 h
8001Eh – 8001Fh	IC Fabrication Date	YDDD h (where Y is the last digit of the year and DDD is the number of the day within the year)
80020h – 80021h	IC Module Fabricator	4252 h
80022h– 80023h	IC Module Packaging date	YDDD h (where Y is the last digit of the year and DDD is the number of the day within the year)
80024h – 80027h	IC Serial Number	A proprietary binary number
80028h – 80029h	IC Batch number	A proprietary binary number
8002Ah	IC Version	11 h
8002Bh	Test ROM Code Version	10 h
8002Ch – 8002Dh	Crypto. Library Version	035C h
8002Eh	DRNG Library Version	02 h
80030h – 8007Fh	Available for customer	All FF h

Table 6: TOE version information

3 Security Policy

The security policy of the TOE is to provide basic Security Functions to be used by the smart card operating system and the smart card application thus providing an overall smart card system security. Therefore, the TOE will implement a symmetric cryptographic block cipher algorithm to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a deterministic random number generator. If the user decides not to use the RSA crypto library the library is not delivered to the user. Hence the

TOE can be delivered with or without the functionality of the RSA crypto library what is resulting in two TOE configurations.

As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during Triple-DES and RSA cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations and against abuse of functionality. Hence the TOE shall

- maintain the integrity and the confidentiality of data stored in the memory of the TOE and
- maintain the integrity, the correct operation and the confidentiality of Security Functions (security mechanisms and associated functions) provided by the TOE.

4 Assumptions and Clarification of Scope

The TOE, the S3CC9GC microcontroller featuring the TORNADO™ cryptographic coprocessor, is a Smart Card integrated circuit which is composed of a processing unit, security components, contactless and contact based I/O ports and volatile and non-volatile memories (hardware). The TOE comprises the hardware of the smart card security controllers, type S3CC9GC and IC Designer/Manufacturer proprietary IC Dedicated Software required for operation. Such software (also known as IC firmware) is mainly used for testing purpose during production only but also provides additional services to facilitate the usage of the hardware and/or additional services including a RSA asymmetric cryptography library and an AIS20 compliant random number generation library. All other software is called Smart Card Embedded Software, which is not part of the TOE.

The TOE is delivered as a hardware unit at the end of the chip manufacturing process (phase 3 of the life cycle defined). At these specific points in time the operating system software is already stored in the non-volatile memories of the chip and the test mode is completely disabled.

The smart card applications need the Security Functions of the smart card operating system based on the security features of the TOE. With respect to security the composition of this TOE, the operating system, and the smart card application is important. Within this composition the security functionality is only partly provided by the TOE and causes dependencies between the TOE Security Functions and the functions provided by the operating system or the smart card application on top. These dependencies are expressed by environmental and secure usage assumptions as outlined in the user documentation.

Within this evaluation of the TOE several aspects were specifically considered to support a composite evaluation of the TOE together with an embedded smart card application software (i.e. smart card operating system and application). This was necessary as Samsung Electronics is the TOE developer and

manufacturer and responsible for specific aspects of handling the embedded smart card application software in its development and production environment. For those aspects refer to part B, chapter 9.2 of this report.

The full evaluation results are applicable only for TOE chips from the semiconductor factory in Giheung, labelled by the production line indicator „14“ as hex.

5 Architectural Information

The TOE S3CC9GC 16-Bit RISC Microcontroller for Smart Card, Version 5 is an integrated circuits (IC) providing a platform to a smart card operating system and smart card application software. A top level block diagram and a list of subsystems can be found within the TOE description of the Security Target [6]. The complete hardware description and the complete instruction set of the TOE is to be found in guidance documents delivered to the customer, see table 5.

The TOE consists of the 19 subsystems (16 hardware / 3 software) as defined in evaluation documentation. For the implementation of the TOE Security Functions basically the components processing unit (CPU) with ROM, EEPROM, RAM, I/O, Deterministic Random Number Generator (DRNG), TORNADO, Clock, Timer / 16-bit Timer and 20-bit Watchdog, Detectors and Security Control, RESET, Address and Data Bus, DES, AES, Power Control, MPU / Memory Protection Unit, Testrom_code, RSA Crypto Library and DRNG Library are used.

Security measures for physical protection are realised within the layout of the whole circuitry. The Special Function Registers, the CPU instructions and the various on-chip memories provide the interface to the software using the Security Functions of the TOE.

The subsystem Testrom_code stored on the chip, is used for testing purposes during production only and is completely separated from the use of the embedded software by disabling before TOE delivery.

6 Documentation

The documentations [11] – [15] are provided with the products by the developer to the customer for secure usage of the TOE in accordance with the Security Target.

Note that the customer who buys the TOE is normally the developer of the operating system and/or application software which will use the TOE as hard-ware computing platform to implement the software (operating system / application software) which will use the TOE.

7 IT Product Testing

The tests performed by the developer were divided into five categories:

(i) Simulation tests: These tests are performed before starting the production to develop the technology for the production and to define the process parameters.

(ii) Qualification tests: These tests are performed after the first production of chips.The tests are performed in test mode. With these tests the influence of temperature, frequency, and voltage on the security functions are tested in detail.

(iii) Verification tests: These tests are performed in normal mode and check the functionality in the end user environment. The results of the qualification and verification tests are the basis on which it is decided, whether the TOE is released to production.

(iv) Security evaluation tests: These tests are performed in normal mode and check the security mechanisms aiming on the security functionality and the effectivness of the mechanisms. The random numbers are tested as required by AIS 20 and fulfil the criteria.

(v) Production tests: These tests are performed at each TOE before delivery. The aim of the production tests is to check whether each chip is functioning correctly.

(vi) Penetration Tests: Penetration Tests are performed to find security flaws in the product.

The developer tests cover all Security Functions and all security mechanisms as identified in the functional specification, the high level design and the low level design. Chips from the production site in Giheung (see part D, annex A of this report) were used for tests.

The evaluators testing effort can be summarised into the following classes of tests: Module tests, Simulation tests, Emulation tests, Tests in normal mode, Tests in test mode and Hardware tests. The evaluators performed independent tests to supplement, augment and to verify the tests performed by the developer by sampling. Besides repeating exactly the developers tests, test parameters were varied and additional analysis was done. With these kind of tests performed in the developer's testing environment the entire security functionality of the TOE was verified. Overall the evaluators have tested the TSF systematically against the functional specification, the high-level design and the low-level design.

The evaluators supplied evidence that the actual version of the TOE with production line indicator "14" as hex in Giheung provides the Security Functions as specified.

Intensive penetration testing was performed at that time to consider the physical tampering of the TOE using highly sophisticated equipment and expertised know-how. Specific additional penetration attacks were performed in the course of this evaluation.

8 Evaluated Configuration

The TOE is the S3CC9GC 16-Bit RISC Microcontroller for Smart Card, Version 5. In the broader sense, the production of the mask sets for the chip production may be looked upon as the procedure for the system generation. The TOE can be delivered in two configurations:

- Smart Card IC S3CC9GC Revision 11,
- Smart Card IC S3CC9GC Revision 11 with Secure Crypto Library V3.5S.

No further generation takes place after delivery to the customer. After delivery the TOE only features one fixed configuration (normal mode), which cannot be altered by the user. The TOE was tested in this configuration. All the evaluation and certification results therefore are only effective for this version of the TOE. For all evaluation activities performed in test mode, there was a rationale why the results are valid for the normal mode, too.

Every information of how to use the TOE and its Security Functions by the software is provided within the user documentation.

9 Results of the Evaluation

9.1 Evaluation of the TOE

The Evaluation Technical Report (ETR), [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components identical with EAL4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body [4, AIS 34]). For smart card IC specific methodology the CC supporting documents

(i) The Application of CC to Integrated Circuits

(ii) Application of Attack Potential to Smart Cards and

(see [4, AIS 25 and AIS 26]) and [4, AIS 31] (Functionality classes and evaluation methodology for deterministic random number generators) were used. The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		Verdict
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Development tools CM coverage	ACM_SCP.2	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Semiformal functional specification	ADV_FSP.2	PASS
Semiformal high-level design	ADV_HLD.2	PASS
Implementation of the TSF	ADV_IMP.2	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Semiformal correspondence demonstration	ADV_RCR.1	PASS
Formal TOE security policy model	ADV_SPM.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Sufficiency of security measures	ALC_DVS.2	PASS
Standardised life-cycle model	ALC_LCD.1	PASS
Compliance with implementation standards	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: low-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS

Assurance classes and components		**Verdict**
Vulnerability assessment	CC Class AVA	PASS
Covert channel analysis	AVA_CCA.1	PASS
Analysis and testing for insecure states	AVA_MSU.3	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

Table 7: Verdicts for the assurance components

The evaluation has shown that

- the TOE is conform to the Smart Card IC Platform Protection Profile, BSI-PP-0002-2001 [9]
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function:
  SF3 – Non-reversibility of TEST and NORMAL modes.
  SF5 – Deterministic Random Number Generator.

The scheme interpretations AIS 26 and AIS 20 (see [4]) were used.

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for

(i) the TOE Security Function SF5 which is the Triple DES encryption and decryption by the hardware co-processor and TORNADO™ coprocessor for RSA Asymmetric Cryptographic Support including RSA Library.

(ii) for other usage of encryption and decryption within the TOE.

For specific evaluation results regarding the development and production environment see annex A in part D of this report.

The code in the Test ROM of the TOE is used by the TOE manufacturer to check the chip function before TOE delivery. This was considered as part of the evaluation under the CC assurance aspects ALC for relevant procedures and under ATE for testing.

The results of the evaluation are only applicable to the TOE as identified in table 5, produced in the semiconductor factory in Giheung, labelled by the production line indicator „14“ as hex within the chip identification number in the EEPROM, and the firmware and software versions as indicated in table 5.

The validity can be extended to new versions and releases of the product or to chips from other production and manufacturing sites, provided the sponsor applies for re-certification or assurance continuity of the modified product, in

accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

9.2 Additional Evaluation Results

- The evaluation confirmed specific results of a previous smart card IC evaluation regarding assurance aspects for the development and production environment. This is outlined in part D of this report, annex A.
- To support a composite evaluation of the TOE together with a specific smart card embedded software additional evaluator actions were performed during the TOE evaluation. The results are documented in the ETR-lite [10] according to [4, AIS 36]. Therefore, the interface between the smart card embedded software developer and the developer of the TOE was examined in detail.

10 Comments/Recommendations

The TOE is delivered to Card Manufacturer and the Smart Card Embedded Software Developer. The actual end user obtains the TOE from the operating system producer together with the application which runs on the TOE.

The Smart Card Embedded Software Developer receives all necessary recommendations and hints to develop his software in form of the delivered documentation.

- All security hints described in [11] and the delivered documents [12], [13], [14] have to be considered.

In addition the following assumptions and requirements concerning external security measures, explicitly documented in the singles evaluation reports, have to be fulfilled:

- Requirement resulting from ADV_LLD:
  Since the hardware cannot guarantee the storage of correct data in case of power loss during memory write operations the software has to implement appropriate measures to check if security relevant data are correctly written.
- Requirement resulting from ADO_DEL:
  - As the TOE is under control of the user software, the chip manufacturer can only guarantee the integrity up to the delivery procedure. It is in the responsibility of the Smart Card Embedded Software Developer to include mechanisms in the implemented software which allows detection of modifications after the delivery.
  - TOEs which failed the production tests are also delivered, as they are inked (marked my black dots) and remain physically on the wafer. The Card Manufacturer has to follow the procedure described in [15] to handle these chips in a secure manner.

In addition the following assumptions and requirements concerning external security measures, explicitly documented in the singles evaluation reports, have to be fulfilled:

- TOEs which failed the production tests are also delivered, as they are inked (marked my black dots) and remain physically on the wafer. The Card Manu-facturer has to follow the procedure described in [15] to handle these chips in a secure manner.

- Requirement resulting from AVA_MSU:
  During an evaluation of the Smart Card Embedded Software the following has to be checked:
  - Application of the security advices given in [12] especially the rec-ommendations for secure usage in [12, chapter 4].
- Requirement resulting from AVA_VLA:
  - The TOE is protected by light sensors against light injection attacks (e.g. with laser). Nevertheless the performed penetration tests show that it is still possible to manipulate a running program with a focussed laser. The Smart Card Embedded Software Developer has to implement sufficient counter-measures in his software to counter such attacks, too.

The Card Manufacturer receives all necessary recommendations and hints to develop his software in form of the delivered documentation.

- All security hints described in [15] have to be considered.

11 Annexes

Annex A: Evaluation results regarding the development and production environment (see part D of this report).

12 Security Target

For the purpose of publishing, the Security Target [7] of the target of evaluation (TOE) is provided within a separate document. It is a sanitized version of the complete Security Target [6] used for the evaluation performed.

13 Definitions

13.1 Acronyms

ACE Advanced Crypto Engine

API Application Programming Interface

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

CBC Cipher Block Chaining

CC	Common Criteria for IT Security Evaluation
DES	Data Encryption Standard; symmetric block cipher algorithm
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
ECB	Electrical Code Block
EEPROM	Electrically Erasable Programmable Read Only Memory
EMA	Electro magnetic analysis
ETR	Evaluation Technical Report
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir, Adelmann – a public key encryption algorithm
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
Triple-DES	Symmetric block cipher algorithm based on the DES
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TSS	TOE Summary Specification

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

- AIS 20 Application Notes and Interpretation of the Scheme (AIS) AIS 20, Version1, Date: 2 December,1999, Status: Mandatory, Subject: Functionality classes and evaluation methodology for, deterministic random number generators, Publisher: Certification body of the BSI, Section II 2, as part of the certification scheme
- AIS 25, Version 2, 29 July 2002 for: CC Supporting Document, - The Application of CC to Integrated Circuits, Version 1.2, July 2002
- AIS 26, Version 2, 6 August 2002 for: CC Supporting Document, - Application of Attack Potential to Smartcards, Version 1.1, July 2002
- AIS 31, Version 1, 25 Sept. 2001 for: Functionality classes and evaluation methodology of physical random number generators
- AIS 32, Version 1, 02 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungs-schema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 36 Version 1, 29 July 2002 for CC Supporting Document, ETR-lite for Composition, Version 1.1, July 2002 and CC Supporting Document, ETR-lite for Composition: Annex A Composite smartcard evaluation, Version 1.2, March 2002

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target, Security Target of S3CC9GC 16-bit RISC Microcontroller for Smart Cards – Project Comanche, Version 1.1, 9. February 2007, Samsung Electronics Co., Ltd.

[7] Security Target Lite of S3CC9GC 16-bit RISC Microcontroller for Smart Cards – Project Comanche, Version 1.0, 13. February 2007

[8] Evaluation Technical Report (ETR), Version 1, 26.02.2007 for the product S3CC9GC 16-Bit RISC Microcontroller for Smart Card, Version 11 (confidential document)

[9] Smart card IC Platform Protection Profile, Version 1.0, July 2001, BSI registration ID: BSI-PP-0002-2001, developed by Atmel Smart Card ICs, Hitachi Ltd., Infineon Technologies AG, Philips Semiconductors

[10] ETR-lite for composition, Version 1, 26.02.2007 for the product S3CC9GC 16-Bit RISC Microcontroller for Smart Card, Version 1 (confidential document)

[11] User's manual S3CC9GC/GW 16-Bit CMOS Microcontroller for Smart Card Version 3.1, 03.2006

[12] Security Application Note, S3CC9GC/S3CC9GW Version 1.5, 18.12.2006

[13] Application Note RSA Crypto Library with TORNADO V3.5S, Version 1.8, 04.07.2006

[14] Application Note DRNG Software Library Version 2.0, 13.12.2006

[15] S3CC9GC Chip Delivery Specification Version 1.2, February 2007.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

a) **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.

b) **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

a) **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.

b) **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

a) **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

b) **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

a) **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Assurance categorisation (chapter 7.5)

"The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”

D Annexes

List of annexes of this certification report

Annex A: Evaluation results regarding development and production environment D-3

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0438-2007

Evaluation results regarding development and production environment

The IT products S3CC9GC 16-Bit RISC Microcontroller for Smart Card, Version 11 (Target of Evaluation, TOE) have been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005), extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance, for conformance to the Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC15408: 2005).

As a result of the TOE certification, dated 01. March 2007, the following results regarding the development and production environment apply. The Common Criteria assurance requirements

- **ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.2),**
- **ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and**
- **ALC – Life cycle support (i.e. ALC_DVS.2, ALC_LCD.1, ALC_TAT.1),**

are fulfiled for the development and production sites of the TOE listed below:

a) Samsung Electronics Co., Ltd. San24, Nongseo-dong, Giheung-gu, Yongin-City, Gyeonggido , 449-711, Korea (Development, Production, Mask House)

b) Samsung Electronics Co., Ltd. San #16, Banwol-Ri, Hwasung-Eup, Gyeonggi-Do, 445-701, Korea (Development)

c) Samsung Electronics Co., Ltd., San #74, Buksoo-Ri, Baebang-Myun, Asan-City, Choongcheongnam-Do, 336-711, Korea (Onyang plant, Delivery)

d) PKL Co., Ltd. Plant, 493-3 Sungsung-Dong, Cheonan-City, Choongcheongnam-Do, 330-300, Korea (Mask House)

The hardware part of the TOE produced in the semiconductor factory in Giheung, Korea, is labelled by the production line indicator „14“ as hex.

For the sites listed above, the requirements have been specifically applied for each site and in accordance with Security Target, Security Target of S3CC9GC 16-bit RISC Microcontroller for Smart Cards – Project Comanche, Version 1.1, 9. February 2007, Samsung Electronics Co., Ltd.

The evaluators verified, that the threats and the security objective for the life cycle phases 2, 3 up to delivery at the end of phases 3 as stated in the Security Target [6] are fulfiled by the procedures of these sites.